Centrale Maths 2 PC 2014 — Corrigé

Ce corrigé est proposé par Gauthier Gidel (ENS Ulm) ; il a été relu par Yvon Vigaud (Professeur en CPGE) et Gilbert Monna (Professeur en CPGE).

Ce sujet est consacré à l'étude des sommes de carrés dans un anneau commutatif A quelconque. Étant donné un entier p non nul, on cherche à établir des formules assurant la stabilité par produit de l'ensemble $\mathrm{C}_p(\mathrm{A})$ des éléments somme de p carrés dans A. Ces formules sont essentielles pour répondre à des questions classiques d'arithmétique comme « quels entiers naturels sont somme de deux carrés ? »

Il utilise de nombreuses parties du programme d'algèbre, principalement les symétries vectorielles, la réduction des endomorphismes et les applications bilinéaires. Mais ce sujet fait aussi appel à des connaissances en arithmétique, en programmation et à des idées classiques analogues à celles utilisées sur les nombres complexes et les entiers de Gauss. L'énoncé comporte cinq parties dont une entièrement consacrée à l'algorithmique.

- La première partie concerne l'étude des symétries et des familles de symétries anticommutant deux à deux.
- La deuxième partie permet d'introduire les quaternions et d'en démontrer certaines propriétés.
- Dans la troisième partie, on réutilise les deux parties précédentes pour l'étude des applications bilinéaires conservant la norme. Il en résulte un théorème dû à Hurwitz qui stipule que les formules recherchées n'existent pas pour $p = 3$.
- La quatrième partie est consacrée à la programmation d'algorithmes pouvant permettre la vérification pratique des résultats démontrés.
- La cinquième partie conclut ce sujet par une preuve du célèbre théorème des quatre carrés. En utilisant les propriétés arithmétiques des quaternions à coordonnées entières et en utilisant les résultats de la partie III, on démontre que tout entier naturel est la somme de quatre carrés d'entiers.

Ce problème est long et comporte des questions difficiles. En particulier la question V.A où l'énoncé conseille même de traiter un cas particulier. Il est extrêmement compliqué de traiter ce sujet en quatre heures. Néanmoins, il recouvre une partie conséquente du programme d'algèbre et permet au passage de se familiariser sur les quaternions.

Indications

Partie I

I.A.1.c Ne pas oublier que les espaces peuvent être triviaux.

I.A.2.b Remarquer que si u est un endormorphisme de E et F un sous espace vectoriel de E alors

$$\dim\big(u(\mathrm{F})\big) \leqslant \dim(\mathrm{F})$$

I.C.1 Montrer qu'un *H-système* est libre.

I.C.3 Penser à utiliser I.B.1.

I.D.1.a Penser à utiliser I.B.1.

I.D.1.b Utiliser le fait que U et S_j anticommutent.

I.D.1.c Majorer p grâce à la définition d'un *H-système* et que $\dim(\mathrm{E}_0) = \dfrac{n}{2}$.

I.D.2 Montrer le résultat par récurrence.

I.E.1 Effectuer des calculs par blocs.

I.E.2 Montrer le résultat par récurrence.

I.E.3 Utiliser le processus de la question I.E.1.

Partie II

II.A.1.a Ne pas oublier que $\mathbb{C}$ est un espace vectoriel réel de dimension 2.

II.A.2 Penser aux matrices $\mathrm{M}(\mathrm{i}, 0)$ et $\mathrm{M}(0, 1)$.

II.A.3.b Utiliser le tableau de la question précédente.

II.B.1.b et c Voir la transformation * comme la composée de la transposition et du passage au conjugué des coefficients et remarquer que ces deux endomorphismes commutent.

II.B.1.d Écrire $\mathrm{N}(qr)e = qr(qr)^*$ et utiliser la question II.B.1.b.

II.B.2.a Utiliser la linéarité de la trace.

II.B.2.b Remarquer que $q = y\mathrm{I} + z\mathrm{J} + t\mathrm{K} \iff q^* = -q$.

II.B.2.c Appliquer la question précédente à un q et r bien choisis puis écrire

$$\mathrm{N}(ac - d^*b)e = (ac - d^*b)(ac - d^*b)^*$$

Partie III

III.A.1 Utiliser pour tous quaternions q et r l'égalité $\mathrm{N}(qr) = \mathrm{N}(q)\mathrm{N}(r)$.

III.A.2 Se servir de la question II.B.2.b en remarquant que pour $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{H}^2$,

$$\left\| \begin{pmatrix} a \\ b \end{pmatrix} \right\|^2 = \mathrm{N}(a) + \mathrm{N}(b)$$

III.B.1.a Utiliser la linéarité du produit scalaire et de u_i.

III.B.1.b Appliquer l'identité précédente avec Y un vecteur de la base canonique de $\mathbb{R}^n$.

III.B.1.c Penser à la relation

$$(a|b) = \frac{\|a+b\|^2 - \|a\|^2 - \|b\|^2}{2}$$

III.B.1.a Utiliser le fait que A_n et A_i anticommutent.

III.B.3 Discuter selon que $m = 1$ ou que $m \geqslant 3$ et se ramener à l'étude de

$$3 \times 2^{d-1} \leqslant d + 1$$

Partie IV

IV.A Utiliser une boucle while.

IV.D Réutiliser les fonctions écrites pour les question IV.A et IV.C.

Partie V

V.A Constater que les applications bilinéaires et les relations associées de la partie III peuvent s'écrire dans un anneau A.

V.B.1.b Remarquer que pour tout x dans $\mathbb{R}$, il existe n dans $\mathbb{N}$ tel que

$$|x - n| \leqslant \frac{1}{2}$$

V.B.1.c Traiter le cas d'égalité de la question précédente.

V.B.2.a Se ramener à

$$p\mathbb{Z} \cap \{0, \ldots, p-1\} = \{0\}$$

V.B.2.b Utiliser le lemme des tiroirs et l'injectivité de ϕ ou alors raisonner sur les cardinaux.

V.B.3.a Faire une disjonction de cas et utiliser l'indication sur des paires d'entiers impairs (dont la somme est toujours paire).

V.B.3.b Effectuer la division euclidienne de x, y, z et t par m.

V.B.3.c Utiliser le fait que $\mathrm{N}(qr) = \mathrm{N}(q)\mathrm{N}(r)$.

I. Symétries vectorielles

I.A.1.a Soit x appartenant à F_s. Alors puisque F et G sont deux sous-espaces vectoriels supplémentaires de E, il existe un unique couple (y,z) appartenant à $\mathrm{F}\times\mathrm{G}$ tel que $x = y+z$. Ainsi,

$$s(x) = s(y+z) = y - z \qquad (s \text{ est une symétrie})$$

de plus, $$s(x) = x = y+z \qquad (x \in \mathrm{F}_s)$$

d'où, $$z = 0 \quad \text{et ainsi} \quad x = y$$

donc $x \in \mathrm{F}$. Si bien que $\mathrm{F}_s \subset \mathrm{F}$.

Réciproquement, soit $x \in \mathrm{F}$. Alors en appliquant la définition de s avec $z = 0 \in \mathrm{G}$, il vient

$$s(x) = x \quad \text{et donc} \quad \mathrm{F} \subset \mathrm{F}_s$$

Finalement par double inclusion $\boxed{\mathrm{F} = \mathrm{F}_s}$

Faisons de même pour G et G_s, Soit $x \in \mathrm{G}_s$. Alors il existe un unique couple (y,z) appartenant à $\mathrm{F}\times\mathrm{G}$ tel que $x = y+z$. Ainsi, il vient

$$y + z = x = -s(x) = -s(y+z) = -y+z$$

Ainsi x appartient à G, donc $\mathrm{G}_s \subset \mathrm{G}$. Soit $x \in \mathrm{G}$, alors en appliquant la définition de s avec $y = 0 \in \mathrm{F}$ il vient $s(x) = -x$. Finalement, par double inclusion

$$\boxed{\mathrm{G} = \mathrm{G}_s}$$

I.A.1.b Soit x appartenant à E. Il existe un unique couple (y,z) dans $\mathrm{F}\times\mathrm{G}$ tel que $x = y+z$. Ainsi,

$$s\circ s(x) = s\big(s(y+z)\big) = s(y-z) = y+z = x$$

d'où, $$\boxed{s\circ s = \mathrm{Id}_\mathrm{E}}$$

L'endomorphisme s a donc pour inverse lui-même.

$$\boxed{\text{L'application s est un automorphisme de E.}}$$

I.A.1.c D'après la question I.A.1.a,

$$Ker(s - \mathrm{Id}_\mathrm{E}) \oplus Ker(s + \mathrm{Id}_\mathrm{E}) = \mathrm{F}_s \oplus \mathrm{G}_s = \mathrm{F} \oplus \mathrm{G} = \mathrm{E}.$$

Dès lors trois cas se présentent :

- Soient $\mathrm{F}_s = Ker(s - \mathrm{Id}_\mathrm{E}) \neq \{0_\mathrm{E}\}$ et $\mathrm{G}_s = Ker(s + \mathrm{Id}_\mathrm{E}) \neq \{0_\mathrm{E}\}$. L'endomorphisme s a donc pour valeurs propres 1 et -1.
- Soit $\mathrm{F}_s = \{0_\mathrm{E}\}$ et alors $\mathrm{G}_s = \mathrm{E}$.
- Soit $\mathrm{G}_s = \{0_\mathrm{E}\}$ et alors $\mathrm{F}_s = \mathrm{E}$.

Il en découle trois conclusions possibles :

> On a respectivement : soit F_s et G_s sont les deux espaces propres, les deux valeurs propres sont 1 et -1. Soit G_s est le seul espace propre, la seule valeur propre est -1. Ou soit F_s est le seul espace propre, la seule valeur propre est 1.